Blockchain for the Security of Internet of Things: A Smart Home use Case using Ethereum

Md. Selim Hossain, Sajjad Waheed, Ziaur Rahman, SK. A. Shezan, Md. Mahabub Hossain

Abstract: Internet of Things (IoT) that has been developed owing toward the merging of various technologies such as instantaneous analytics, machine learning, artificial neural network, product sensors and implanted systems, etc. It also stages a significant part in multiple applications which are a smart city, smart home, agricultural, health monitoring, tourism, transportation, communication, business, education, etc. The security concern associating IoT has to be situated in the direction to attract the research community due to its immensely growing application in our daily life. Since it is light-weight nature, the security mechanism needs changes apart from comprehensive web security. PKI based certificate driven techniques, which in some instances seem not appropriate on the way toward encounter IoT challenges, e.g., as real-time effectiveness, costs, and performance from the security perspective. However, Blockchain has mind-blowing potentials to peer with the IoT aiming to build trust, transparency, and security. Its distinct properties, such as distributed behavior, immutability, and consensus mechanism, can stimulate and improve the rapidly growing IoT system through meaningful integration. We propose to address a practical smart home use case scenario using Ethereum Blockchain to improve IoT security. Public type and smart contract oriented Ethereum Blockchain are adaptable to enhance IoT security remains individual of the contributions that we claim throughout this research work.

Keywords: IoT, Blockchain, Ethereum, Smart Contract, Safety and Privacy, Solidity Programming, Smart Area, etc.

I. INTRODUCTION

Internet of Things (IoT) has been obtaining acceptance gradually. It shows the way in the progress of numerous submissions such as smart city, smart home, agricultural, health monitoring, tourism, transportation, communication, business,

Md. Selim Hossain*, Khwaja Yunus Ali University, Enayetpur, Sirajganj-6751, Bangladesh. Email: selimtee@gmail.com

Sajjad Waheed, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. Email: swaheed.iu@gmail.com

Ziaur Rahman, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. Email: rahman.ziaur@rmit.edu.au

SK. A. Shezan, School of Engineering, RMIT University, Melbourne, Australia, Email: shezan.arefin@rmit.edu.au

Md. Mahabub Hossain, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.
Email: im.mahabub@gmail.com

education, banking sector, other transaction-based matters, etc. The more use of IoT devices, the more the takes to be ensured security and privacy in our everyday life. Blockchain, the new era of technology is considered as anemerging concepts and technological development. A Blockchain is an ordinal register system that is applicable in a distributed manner such as peer to peer system [1]. We recommend a new Ethereum constructed Blockchain system in this research work to integrate with the IoT structure to confirm the security issues of these devices. Our experimental results based on the Ethereum platform and simulation have been performed to the updated version of the packet tracer. Due to the extensive use of IoT, security concern is quiet under the development stage, that means a considerable amount of works wants to be done for enhancing the safety and confidentiality of this technology. A lot of employment has been completed in the improvement of IoT that consist of solicitation development, safekeeping, confidentiality, its connectivity, procedures construction, heterogeneity, sustainability, etc. IoT devices will supplementary increase to an extent 30 billion utilizing 2020 and completed 60 billion by the accomplishment of 2025 [14]. This massive number of new appliances does not come without the cost matter. Trojans or Viruses are nearly illustrations of Denial of Services (DoS) [15]. In such cases, intruders develop a Virus which is programmed to gather in a specific manner to terminate the host technique.

II. TECHNICAL PRELIMINARIES: SMART HOME

A Smart Home (S.H.) denotes a dwelling prepared through a communiqué net, advanced domestic devices, applications, and sensors that tin is remotely opened, checked, and measured and that offer facility retorting to the inhabitants' requirements [5]. Primarily, a smart home was well-defined utilizing numerous appellations, such as a home network, a digital home, home computerization, and artificial intelligent based home. It has been inclined to an amalgamation of IoT and a situation-aware smart home. A smart home is a progressive procedure of old-style home computerization. S.H. was predisposed by home computerization, communiqué devices to link with the variability of facilities at home, guaranteeing financial, protected, and relaxed procedures of the house [6]. Consequently, S.H. deal was being used to accomplish ecological structures alike lighting and central heating [3]. Due to technical progress, S.H. service displays manipulator movement and the interior atmosphere at home. Furthermore, S.H. facilities are accomplished the difficulties and requirements of a manipulator. Newly, S.H. facilities are developing as they method artificial intelligence.

Moreover, China S.H. manufacturer Xiaomi is scheduling to mark the S.H. marketplace as a share of its enduring apparition. Consequently, S.H. facilities are emerging and multiplying by accepting IoT and artificial intelligence.

To the comprehensiveness of S.H. facility have been paid suggestively. Nevertheless, as research on commercial and manipulator perceptions for market renaissance was deficient, more training is obligatory to inspire the propagation of S.H. accommodations.

III. INTERNET OF THINGS

Kevin Ashton anticipated the IoT at Massachusetts Institute of Technology in 1999. IoT devices involved outspreading the Internet connectivity outside usual plans like as smartphones, desktops, laptops that be situated unadventurously. IoT devices have been recognized for subsequent ambitions. Firstly, the increasing connectivity of sensor-based systems. Secondly, computers would develop independent, ready to accumulate information [7]. Moreover, IoT characterizes a broader change to the dream of worldwide figuring [8]. Presently critical requests such as conventional vehicles and modern structures are interlinked of millions of devices [9]. IoT is a platform by attaching the system of numerous objects like as radio-frequency, documentation tags, sensors, actuators, mobile phones, thermometers and other comparable devices [5].

IV. BLOCKCHAIN

Here remains a problem in communication systems that is difficult when no authentication nor inspection mechanisms are providing, especially nearby stands a deal with thoughtful information; for example, economic dealings with virtual exchanges. Satoshi Nakamoto demonstrated two radical conceptions in 2008, which have had a great outcome. The popularity of these ideas has moved out even supplementary than the cryptocurrency that is called Blockchain. Blockchain permits dealings to be confirmed by an assemblage of untrustworthy actors. This technology bids a distributed ledger system, unchallengeable, apparent, protected and auditable record system. Blockchain can be referred wholly and willingly, permitting admittance to all dealings that have followed the original contract of the system subsequently, and can be substantiated and organized through slightly. Blockchain protocol assemblies the information in a sequence of blocks, where each Block supplies a set of Bitcoin contacts performed at a duration. Here, Blocks remain connected by an orientation to the former Block or previous hash value, establishing a chain.

V. WHY BLOCKCHAIN

One of the important features of BC is immutability means somewhat that will not be altered. These remaining unique of Blockchain features that help to confirm that the technology will continue as it is an everlasting, permanent network. The planned in the direction of being scattered and harmonized across networks which mark it ideal for multi-organizational systems such as supply chains or financial associations is known as distributed behavior [20]. Next one is Enhanced Security [10]; Cryptography lays another layer of security for customers due to the Decentralization. We can define another one is the smart contracts which the categories of dealings individual can convey ready to be

situated approved between applicants in early payment and warehoused. In the Blockchain as well as Consensus: Before executing a deal, here essential stay a contract between all relevant parties that the transaction is legal by registering the sale belongs to an agreement. This procedure is known as Consensus. Chronological and Time Stamped is a numerical register storing apparatus anywhere individually transaction or event is time-stamped (chronological) stylish a protected way by the hashed value. The critical feature is Irreversible; Hashing is relatively composite as well as the is impossible to modify or reverse it. So, minor deviations are not extravagance in the method and Decentralization. Applications demand Decentralization when here stays not a trusted centralized system. The further away we can say Peer to Peer Exchange; Communications among peers at a node level are not very common except for specific applications. Micro-Transaction Collection; IoT transactions maintain traceability for auditing purposes. In these situations, a side chain may be useful. Some other apps do not need to store every collected value. For example, in remote agricultural monitoring where communications are expensive. A local system may well accumulate and stock the data, and once a day it transmits to process the information.

VI. BASIC FUNCTION OF BLOCKCHAIN

Blockchain is a cardinal record system where information is collective among the network of peers. We mentioned it beforehand; it reflects the central involvement of Bitcoin, meanwhile, is explained as a longer-lasting economic problem acknowledged as the double-spend tricky. The explanation was being projected by the Bitcoin group contained regarding the compromise of maximum withdrawal nodes, by which the validity of transactions to the Blockchain is checked. Blockchain concept has been given below.

Block 1(1 MB)	Hash value
Transaction Data	2346ad27d7568ba9896f1b7da6b5991251debdf2
Previous Hash Value	bb045d7c0290e97a51e85c6eef8e1c8961f47d43
Generated Hash Value	b6ae46886c733f7c1c9e815fd42037ef2fdba52c

Block 2(1 MB)	Hash value
Transaction Data	f32b67c7e26342af42efabc674d441dca0a281c5
Previous Hash Value	b6ae46886c733f7c1c9e815fd42037ef2fdba52c
Generated Hash Value	bb045d7c0290e97a51e85c6eef8e1c8961f47d43
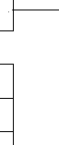
VII. TYPES OF BLOCKCHAIN

Blockchain provides a competent application of public key cryptography and hashing that can be prolonged for digital identity possession and supports safeguarding the integrity and authenticity of identity-based archives. It aids simplifying permission-based record distribution with smart deals. Different types of Blockchain has been categorized conditional on the succeeded information, on the accessibility of such information, and on come again, actions can be achieved through users. In this way, we can differentiate amid public and private,

and permission granted and permission-less Blockchain technology. A figure of types of Blockchain has been provided below has been provided below:
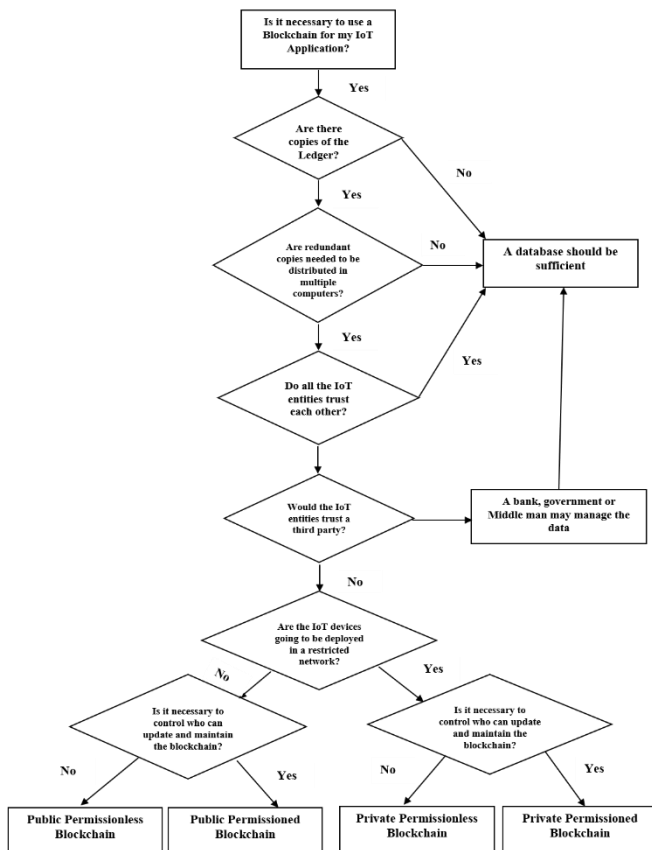

Fig. 1: Types of blockchain technology [20]

Table- I: Comparison of different blockchain systems [8]

	Application	Smart Contract Execution	Smart Contract Language	Consensus
Hyper ledger	General	Dockers	Golang, Java	PBFT
Bitcoin	Crypto-currency	Native	Golang, C++	PoW
Litecoin	Crypto-currency	Native	Golang, C++	PoW (memory)
Ethereum	General Applications	EVM	Solidity, Serpent, LLL	PoW
Quorum	General Applications	EVM	Golang	Raft
Ripple	Digital Assets	-	-	Ripple Consensus
Corda	Digital Assets	JVM	Kotlin, Java	Raft

VIII. BLOCKCHAIN AND IOT APPLICATIONS

Smart Home has converted the radical pecking order of achievement trendy the inhabited chairs which is foretold Smart households is develop as smartphones and automated system combinations of sensors [19]. IoT in Industry: IoT grips inordinate possible aimed at superiority governor and sustainability of the industry, chasing properties, actual evidence transformation, automated delivery which will raise the overall efficiency. IoT for Health Care: Investigation displays IoT trendy medical sector resolve the vast in the recent centuries [13]. Medical sector IoT remains

intended at permitting users near living an improved lifetime through wearing associated devices. IoT for Agricultural Sector: Administrations remain serving agriculturalists by providing advanced techniques as well as exploration on growing food production [11]. The growing field is improved reappearance scheduled asset of detecting aimed at mud wetness which is ideal is known as smart farming. IoT in Transportation: Traffic congestion, GPS procedure from city vehicle stays a city-wide opinion of the communal transportation structure through the accomplishment of calculating vehicle entrances, transit times and direction cramming arranged an ordinal record of the urban [12][14].
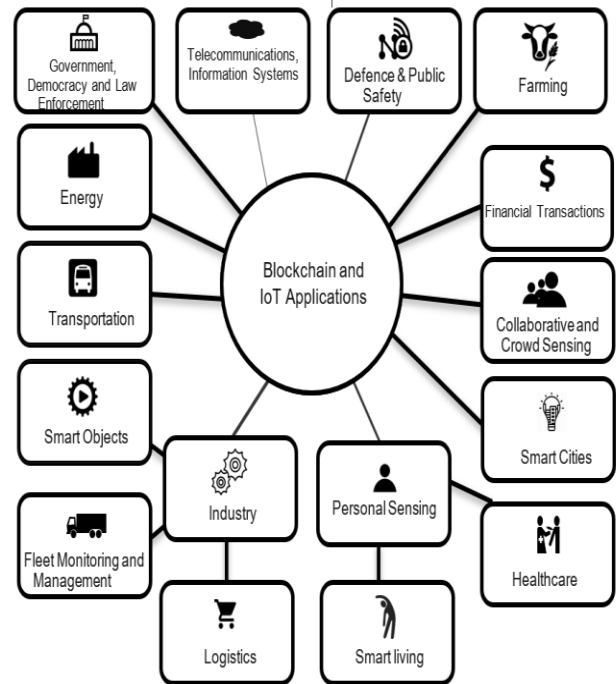

Fig. 2: Blockchain and IoT applications [18][19]

IX. SMART CONTRACTS

The procedure of computation implemented when a transaction is achieved recognized by way of a smart contract. The inputs, outputs, and states exaggerated by the quick contract execution stay on by each node. Blockchains have built-in intelligent contracts that deploy transaction logic in a crypto-logic manner [4][11]. For example, we can say that the integrated smart contract first confirms transaction inputs by checking the validation process. Next, it authenticates the balance of the output addresses matches that of the contributions. Finally, it applies changes to the states.

X. CONSENSUS

Consensus apparatuses are accountable for the truthfulness of the data controlled in Blockchain while protecting against double-spend occurrences and an essential portion of Blockchain technology [2]. The final goal line is toward a consensus in a scattered network without central establishments and with members who do not share unavoidably faith individually.

Table- II: Comparison of different consensus protocols of blockchain technology [16][17]

PBFT Based	Private	Hyperledger uses the original PBFT. Tendermin enhances it by assigning unequal weights to votes.
Ripple	Ripple Federated	Ripple reimbursement structure suggests a different of PBFT anywhere the nodes fit interconnecting collections
Proof of Work (PoW)	Public	Bitcoin uses pure Proof of Work which leads to scalability issues. Bitcoin-NG, Byzcoin separate leader election from transaction validation in PoW.
Proof of Stake (PoS)	Public	Tendermint usages Proof of Stake (PoS) in which nodes stay to create new Block is determined by its stake in the Blockchain
Proof of Authority (PoA)	Private	Parity uses Proof of Authority (PoA) in which pre-defined nodes remain reliable authorities and users can suggest the next blocks
Test of Elapsed Time (PoET)	Private	Test of Elapsed Time (PoET) in which each node runs trusted hardware that generates random timers. The first node where the regulator has perished can recommend the next Block.

XI. PROPOSED METHOD

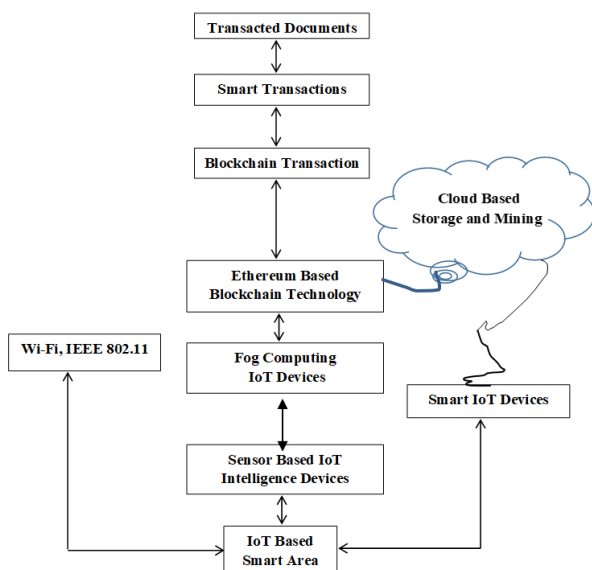Conceptual Architecture of Proposed Model Using Ethereum-Blockchain

Fig. 3: Block diagram of proposed concept

XII. WORKING PRINCIPLE OF PROPOSED MODEL

Now, we are going to describe the proposed model individually, Wi-Fi, IEEE 802.11, which provides Internet connectivity to the IoT plans to exist in a smart home. It is also used for communicating the cloud-based server and cloud-based storage. Moreover, some local storage will be used to store the IoT transacted data. Fog Computing IoT plans that will be used as a filter and sensed the usable data. Ethereum Based Blockchain system which includes the Cloud-based storage and mining system, which will be provided by Oracle Corporation or that these types of service will be supplied by other service-based organization such as Amazon or Alibaba. The procedure of a transaction with other transactions are called blocks. Miner is used to verifying the dealings inside the Block by following a set rule. Miners also check the validation of the newly added Block. A reward system is provided toward the miners to legalize the Block. After verification of the transactions, it is warehoused in the Blockchain. Solidarity programming language is used to modify the permission to access the network whether it private Ethereum based blockchain system. Though Ethereum stands a public and permission-less Blockchain system, we will try to make the permission. However, it may be private Blockchain technology by solidarity programming language. Miner will be used to evidence the validity of the transaction.

XIII. PROPOSED ALGORITHM

Algorithm 1: Algorithmic Structure of Proposed Concept
input: α: IoT devices, users, α-D: solidarity databases for α: IoT system
output: the mining requirement of IoT devices, report of miners and another dataset
for each α: IoT device! = solidarity databases (α) | users do
β= register (users and IoT devices in databases) | reject (users and IoT devices)
if (condition (β) <= below the standards of IoT devices) then
mine= mine+ requirement of IoT devices
send the report(mine) to a miner
else
function (proper IoT action)
end
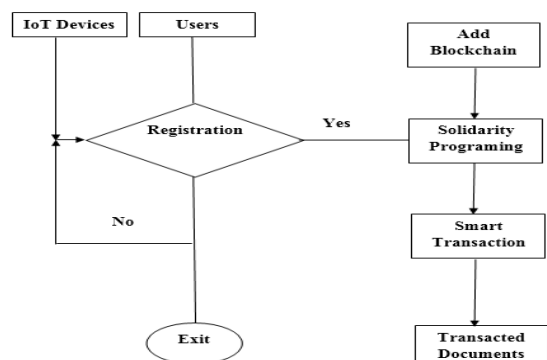
XIV. DIAGRAM OF PROPOSED ALGORITHM

Fig. 4: Diagram of proposed algorithm

XV. WORKING PRINCIPLE OF PROPOSED ALGORITHM

When Users or IoT plans are linked in a smart area, the devices must be registered in the Ethereum platform where solidarity programming coding will be applied to add users or IoT devices. If new users or IoT devices will not log in such a system, this user or IoT devices will be rejected from that smart system. When users or devices add to the smart home system, the IoT device transaction mechanism will be function according to the programming instruction of solidarity programming, and the Blockchain mechanism will be further added to this transaction. Transacted documents will be stored in the local databases as well as cloud-based according to the demand of that system. But we suggest in our research paper to save the IoT generated data to the local database, and Blockchain related data will be separately stored to the cloud server by using local internet service.

XVI. EVALUATION AND RESULT ANALYSIS

Experiment Setting:

1) Dataset: This paper uses packet tracer and solidarity programming language. By using packet tracer and solidarity programming language, some data and records of transactions have been taken. The experimental data have been shown in the result and evaluation section.

2) Operating Environment and Parameter Configuration: The experimental environment in this paper is Cisco Packet Tracer (Version-7) and http://remix.ethereum.org/ online IDE for solidarity programming language. Hardwire environment is 1.80 GHz Intel(R) Core (T.M.) i5-8265U CPU, 15 G.B., Win 10 system of 64 bit. The parameters that are used during the experiment have been given in Table.

A. Simulation scenario of research work in packet tracer (version 7)

Smart Things are corporal substances that can be attached to the record-keeping attendant or home-based entrance over the network line mechanism, which is called registration or connected to the server. The Internet of Everything's (IoE) can straight catalogue on a Home-grown entrance or server devices can be configured with the IoE services. For example, in a smart area, Fan touches wind speed, humidity and ambient temperature can be controlled by IoT based mechanism. A simulation has been performed in the packet tracer updated version that has been shown below.
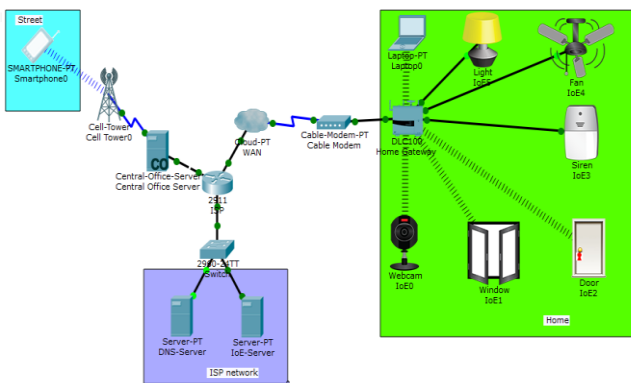

Fig. 5: Simulation scenario of a smart area using IoE devices

By logging in to smart devices such as phones or laptops, we can control the IoE devices from anywhere, anytime and anyplace, which is called the Smart Home system.

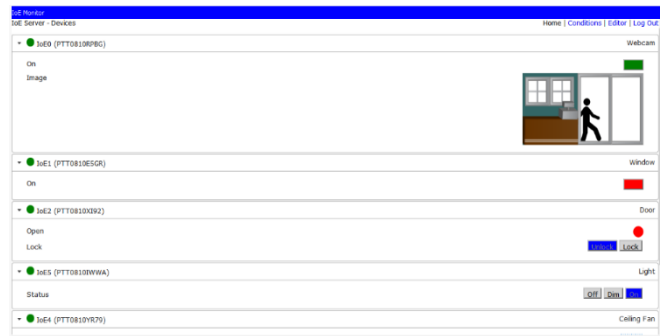### B. Remote monitoring of IoE devices simulated in packet tracer.

Fig. 6: Remote monitoring of IoE devices

XVII. RESULT ANALYSIS AND DISCUSSION

A Delay times that splits the incidence of two proceedings. A network established that the program would not be broadcast but would have a short time delay assembled into the transmission to permit. For example, if we use seven devices then delay is times 10, 20, 30, 40, 50, 80, 100 and 110

Table- III: Delay times after adding devices in the nodes

Devices	1st	2nd	3rd	4th	5th	6th	7th
Delay	10	20	40	50	80	100	110
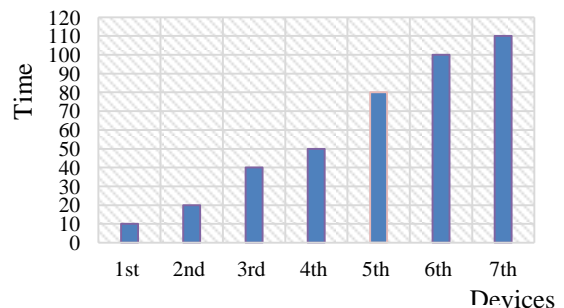
Fig.7: Delay time of IoT Devices

Fig. 8: Continuous curve of delay

Blockchain for the Security of Internet of Things: A Smart Home Use Case using Ethereum
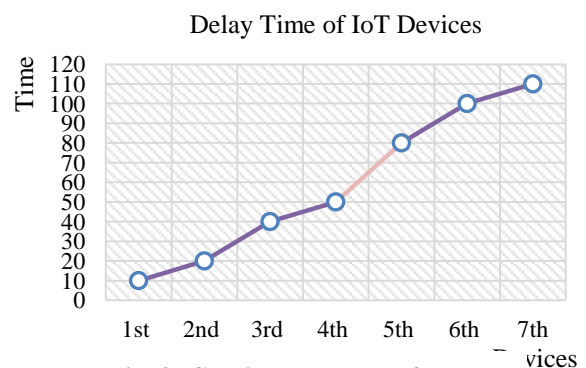
A. Throughput and Latency

The latency of a transaction t as the time is taken for it to be included in a block. Note that this does not necessarily correspond to the inclusion time of t, as Ethereum cannot deterministically define the inclusion of a transaction as several appended blocks or confirmations. Throughput is an amount of how various components of information a structure can procedure in a specified volume of period. It is applied generally to schemes ranging from numerous aspects of network systems to administrations. Peak performance with eight servers and eight concurrent clients where latency and throughput have been found 92 seconds and 294 seconds, respectively. Graphical representation and Tables of d latency and performance have been provided below:

Table- IV: Throughput and Latency

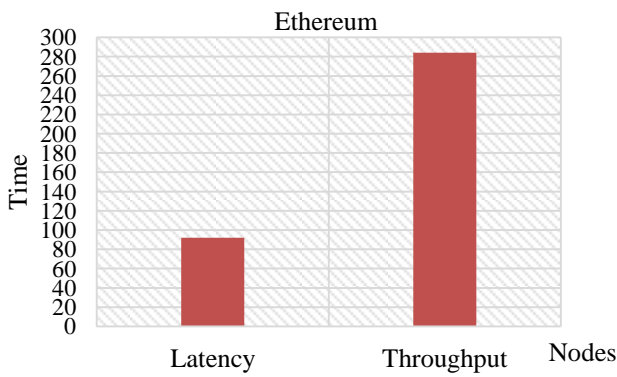| Feature's Name	Latency	Throughput
Time(S)	92	284

Fig. 9: Throughput and Latency of Ethereum

Table- V: Output of solidarity programming

transaction hash	0x548e1c82dd9fd01b4c36330b420d1a12de1db04a306251a452 429062bb7efd79
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	MyContract.people(uint256) 0xef55bfac4228981e850936aaf042951f7b146e41
transaction cost	30841 gas (Cost only applies when called by a contract)
execution cost	9377 gas (Cost only applies when called by a contract)
hash	0x548e1c82dd9fd01b4c36330b420d1a12de1db04a306251a4524 29062bb7efd79
input	0x9e7...00001
decoded input	{"uint256 ": "1"}
decoded output	{"0": "uint256: _id 1102050", "1": "string: _source 29062bb7efd79", "2": "string: _destination 51f7b146e41", "3": "string: _active on", "4": "string: _timestamps 384", "5": "string: _visibilitysetting off"}
logs	[]

The above output is the registration process in the solidarity databases using the Ethereum programming language where the transaction hash will generate according to the coding structure of the program. The hash value that has been mentioned in the next following line where 0xca35b7d915458ef540ade6068dfe2f44e8fa733c, is the origination of the transaction in Ethereum wavelet platform and 0xef55bfac4228981e850936aaf042951f7b146e41 is the destination hash value. This may be a hash value of the server address. Transaction cost from one IoT devices to other IoT devices can be measured by gas value. We also consider the ether value of this transaction where the transaction cost will be limited in accordance with the user or programmer. Execution cost is considered by gas value or ether value where charges first put on when termed by agreement. Some other transaction outputs are provided below with each transaction identification.

Table- VI: Output of transaction using solidarity

status	0x1 Transaction mined and execution succeed
transaction hash	0xb99154b366893690f4edf3f3097cf2e016b626b00b8c22d1a8a3adb2c278a513
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	SHSP.send(address,uint256)0x0dcd2f752394c41875e259e00bb44fd505297caf
gas	3000000 gas
transaction cost	50740 gas
execution cost	27868 gas
hash	0xb99154b366893690f4edf3f3097cf2e016b626b00b8c22d1a8a3adb2c278a513
input	0xd06...00001
decoded input	{"address receiver": "0x0DCd2F752394c41875e259e00bb44fd505297caF", "uint256 amount": "1"}
decoded-output	{}
logs	[{"from": "0x0dcd2f752394c41875e259e00bb44fd505297caf", "topic":"0x3990db2d31862302a685e8086b5755072a6e2b5b780af1ee81ece35ee3cd3345", "event": "Sent", "args": {"0":"0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c", "1": "0x0DCd2F752394c41875e259e00bb44fd505297caF", "2": "1", "from": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c", "to": "0x0DCd2F752394c41875e259e00bb44fd505297caF", "amount": "1", "length": 3 } }]
value	0 wei

XVIII. DESCRIPTION OF MINING OPERATION

The process of a transaction with other transactions is called blocks. Miner is used to verifying the transactions within the block by following a set rule. Miners also check the validation of the newly added block. A reward system is provided to the miner to validate the block. After verification of the transactions, it is stored in the Blockchain.

Logs information can't be seen due to the inheritance property of Ethereum Blockchain technology. The server or Miner will also responsible overall transaction process of this mechanism of a smart home. From the above Miner address that is "0xca35b7d915458ef540ade6068dfe2f44e8fa733c" will be used to store all the requirement of this transaction and every transaction of IoE device will be occurred according to the time-stamped manner. If the transaction can't occur in the time stamp manner of devices.

XIX. LIMITATIONS OF PROPOSED SYSTEM

In the Ethereum based Blockchain technology, the transaction will occur by cryptologic manner where logs are not accessible and can't be altered. We can't access the logs information of this Ethereum based Blockchain transaction. The technologies sector will be affected by scalability and storing as well as to move from the existing technology to the Ethereum based Blockchain technology. The number of transactions that can be made in a given time manner where the miner must perform the calculation with the help of a solution-based computer. The amalgamation of Ethereum based Blockchain technology with IoT must be located, captivating into account has been recognized. Crypto-currencies have been oppressed by persons to yield partial benefit of this. The incorporation of the IoT and Blockchain will significantly progress the practice of Blockchain, in such a technique as to launch crypto-currencies on the same level as the current fiduciary transaction. Smart Conventions originated with the similar compensations of immutability as Blockchain. Though this immutability established values in terms of security and there are few limitations originated as well as they are approximately incredible to alteration. Even the least error in cryptogram can turn out to be expensive and time-consuming to accurate once when the smart agreement is positioned to implement. While the eradication of third gatherings remains a hypothesis that takes set for Blockchain and original indenture, which is no way to eliminate them.

XX. CONCLUSION AND FUTURE SCOPE

The IoT and Blockchain amalgamation will importantly affect the system in such a technique to inaugurate crypto-currency on the matching neck and neck as the current fiduciary currency. In our research, we have tried to add Ethereum based Blockchain with IoT devices to make sure the safekeeping and concealment of these IoT devices. This research is not only applicable to smart home but also has a tremendous amount of execution where IoT projects can be implemented to make the imaginative world. We can conclude that Ethereum based Blockchain with the integration of IoT that is our proposed work is still in its initial stage. Beyond the early stage of Blockchain-based IoT progress and organizations were more extensive in terms of use. These will necessitate the additional scientific exploration developments to address the precise difficulties. Moreover, in this factor, the partnership of research groups, public-private organization, and government to turn the existing system to the next generation information platform. We plan to remove the limitations, and challenges of this research and partially practical implementation of this proposed model to increase the security and privacy of smart devices.

REFERENCES

1. Ana Reyna, R.A., Cristian Martín, C.M., Jaime Chen, C.J., Enrique.: Soler, S.E., & Manuel Díaz, D.M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems 88 173–190
2. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Int. Things J.,5, 1184–1195
3. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P. (2018): Enabling Blockchain Innovations with Pegged Sidechains. Available online: https://www.blockstream. com/sidechains.pdf.
4. Yli-Huumo, J., Ko, D., Choi, S., Park S., & Smolander, K. (2016): Where Is Current Research on Blockchain Technology. A Systematic Review. in PLOS ONE vol.11, no. 10, pp.1-27
5. Rahman, A. Hossain, S., Rahman, Z. and Shezan, SK. A. (2019): Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain. International Journal of Advanced Technology and Engineering Exploration, Vol 6(61).
6. Ongaro, D. & Ousterhout, J. K. (2014).: In search of an understandable consensus algorithm. In Proceedings of the USENIX Annual Technical Conference (USENIX ATC), Philadelphia, PA, USA, pp. 305–319.
7. Lamport, L.: Paxos made simple, fast, and byzantine in Proceedings of the 6th International Conference on Principles of Distributed Systems (OPODIS). Reims, France, pp. 7–9.
8. Brown, R. (2016): Introducing r3 cordatm: A distributed ledger designed for financial services. R3CEV blog.
9. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, S. and Yaqoob, I. (2017): Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges, in IEEE Access, vol. 5, pp. 5247-5261, Mar. 2017
10. Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque and Antônio A. de A. Rocha. (2018): A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Article ID 9675050, pp. 27
11. Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. in IEEE Access, vol. 4, pp. 2292-2303, May 2016
12. Wu, Z., Meng and Z., Gray, J. (2017): IoT-Based Techniques for Online M2M Interactive Itemized Data Registration and Offline Information Traceability in a Digital Manufacturing System. in IEEE Transactions on Industrial Informatics, vol. 13, no. 5, pp. 2397-2405.
13. Kafle, Y. R., Mahmud, K., Morsalin, S. and Town, G. E. (2016): Towards an internet of energy. in Proceedings of the IEEE International Conference on Power System Technology (POWERCON), Wollongong, Australia, 28 Sep.-1 Oct. 2016, Pages 1-678
14. Lomotey, R. K., Pry, J., Sriramoju, S., Kaku, E. and Deters, R. (2017): Wearable IoT Data Architecture. in Proceedings of the IEEE World Congress on Services (SERVICES), Honolulu, United States, 25-30 June.
15. US Computer Emergency Readiness Team. (2016): Heightened DDoS Threat Posed by Mirai and Other Botnets. alert TA16-288A, 14 Oct. 2016 (revised 30 Nov. 2016.
16. Zbierski, M. (2015): Parallel byzantine fault tolerance. in Soft Computing in Computer and Information Science. Springer, pp. 321–333.
17. Zhao, W. (2016): Optimistic byzantine fault tolerance. International Journal of Parallel, Emergent and Distributed Systems. vol. 31, no. 3, pp. 254–267
18. Aazam, M. and Huh, E-N. (2014): Fog computing and smart gateway-based communication for cloud of things. Proceedings of the 2nd International Conference on Future Internet of Things and Cloud, FiCloud-2014, Barcelona, Spain, pp. 27–29
19. Blanco-Novoa, O., Fernández-Caramés, T. M., Fraga-Lamas and P., Castedo, L. (2017): An Electricity-Price Aware Open-Source Smart Socket for the Internet of Energy", in Sensors, vol. 17 (3), no. 643, pp. 1–34.
20. Fernández-Caramés, T. M. Fraga-Lamas, P. (2018): A Review on the Use of Blockchain for the Internet of Things, DOI 10.1109/ACCESS.2018.2842685, IEEE Access

AUTHORS PROFILE

Md. Selim Hossain, has been working as a Lecturer in Department of Computer Science and Engineering at Khwaja Yunus Ali University, Sirajganj, Bangladesh. He completed his B.Sc. degree on Telecommunication and Electronic Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh and M.Sc. (Engg.) on Information and Communication Technology from Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. His main research interest is based on IoT, Blockchain, Cryptography and Network Security.

Sajjad Waheed, currently works as a Professor at the Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. He is a Ph.D. holder in the field of Computer Engineering from Istanbul University, Turkey. He has research interest in Machine Learning, Artificial Intelligence, Artificial Neural Network Data Mining and Blockchain Technology

Ziaur Rahman, is currently a PhD Candidate at RMIT University, Melbourne, and an assistant professor of the Department of ICT, MBSTU, Bangladesh. He was graduated from Shenyang University of Chemical Technology, China, in 2012 and completed Masters in Computer Science from IUT, OIC in 2015. His research interests are Blockchain, IoT, and Cybersecurity.

Shezan Arefin, is the researcher of Electrical and Electronic Engineering Dept. of RMIT University, Melbourne, Australia. He was a lecturer of Electrical and Electronics Engineering Dept. of Uttara University, Dhaka, Bangladesh. He received his Master of Engineering degree from University of Malaya, in 2016. Moreover, he received his Bachelor of Engineering degree in Electrical Engineering and Automation from Shenyang University of Chemical Technology, China, in 2013. His research interests are Microgrid, HRES, Solar Energy, Wind Energy and etc.

Md. Mahabub Hossain, is currently working as an Associate Professor and Head in Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh. He completed his Ph.D. in Semiconductor and Display Engineering, School of Electronics Engineering, Kyungpook National University, South Korea and M. Sc. in Applied Physics & Electronic Engineering and B. Sc. (Honours) in Applied Physics & Electronics, Rajshahi University, Bangladesh. His main research interest is based on Micro/Nanosystems design, materials, and micro/nanofabrication: MEMS/NEMS sensors; Micro actuators; Optical MEMS; Micro adaptive optics; Optofluidics